

Listing and Amendments to the Claims

This listing of claims will replace the claims that were published in the PCT Application and annexed to the International Preliminary Report on Patentability:

1. (original) A method for controlling access by a user terminal to a communications network comprising the steps of:
 - receiving from the user terminal a request to access the communications network;
 - transmitting to the user terminal an identity request message;
 - receiving from the user terminal, if the user terminal utilizes a predetermined authentication protocol, a response to the identity request message;
 - determining whether the user terminal uses the predetermined authentication protocol in response to the response to the identity request message;
 - selecting an authentication mechanism compatible with the user terminal upon determining the user terminal is not compatible with the predetermined authentication protocol, for allowing user terminal access to the communications.
2. (currently amended) The method according to claim 1, wherein the user terminal comprises a mobile terminal and the communications network comprises a wireless local area network ~~WLAN~~ wireless local area network that complies with the IEEE 802.11 standards.
3. (currently amended) The method according to claim 2, wherein the selecting step includes selecting an appropriate authentication server ~~couples~~ coupled to the ~~WLAN~~ wireless local area network in response to the determination.
4. (currently amended) A method for controlling mobile terminal access to a wireless local area network (~~WLAN~~), comprising the steps of:
 - receiving from the mobile terminal a request to access the ~~WLAN~~ wireless local area network;
 - transmitting to the mobile terminal an identity request message;

receiving from the mobile terminal, if the mobile terminal utilizes an ~~FWWW~~
IEEE 802.1x protocol, a response to the identity request message;

determining whether the mobile terminal is IEEE 802.1x compliant in
response to the response to the identity request message; and

selecting an authentication mechanism, compatible with the mobile terminal
in response to the determination, for allowing user mobile terminal access to the
~~WLAN~~ wireless local area network.

5. (currently amended) The method according to claim 4, further
comprising the steps of, if the mobile terminal is IEEE 802.1x compliant, transmitting
an authentication request to an authentication server and receiving an authentication
response utilizing the IEEE 802.1x protocol, and controlling mobile terminal access
to the ~~WLAN~~ wireless local area network in response to the authentication response.

6. (original) The method according to claim 4, further comprising the
steps of, if the mobile terminal is not IEEE 802.1x compliant, redirecting an
authentication request to an HTTP server for utilizing a browser based
authentication.

7. (original) The method according to claim 6, further comprising the
step of configuring a packet filtering module to redirect the authentication request
to the HTTP server.

8. (currently amended) The method according to claim 7, further
comprising the step of maintaining state information in the ~~WLAN~~ wireless local
area network for use by the packet filtering module and the HTTP server.

9. (original) The method according to claim 8, wherein the state
information includes one of a first state indicative of ongoing authentication
process, a second state indicative of authentication failure, a third state indicative
of authentication success, and a fourth state indicative of a non IEEE 802.1x
mobile terminal.

10. (original) An access point in communication with a terminal device in a wireless local area network, comprising:

a means to determine whether the terminal device utilizes an IEEE 802.1x protocol and, if the terminal does not utilize said protocol, then the access point employing an authentication means compatible with the terminal device otherwise the access point employing an IEEE 802.1x protocol.

11. (currently amended) The access point in claim 10, wherein the means to determine includes communicating to the terminal device a Request-Identity EAP extensible authentication protocol packet and if the mobile terminal utilizes the IEEE 802.1x protocol the access receives a Response-Identity EAP extensible authentication protocol packet.

12. (currently amended) The access point in claim 11, further comprises the means to configure an IP internet protocol packet filtering to redirect the device HTTP request to a local server if the terminal device does not utilize said protocol.

13. (currently amended) The access point in claim 10, further comprises means to communicate IEEE 802.1x protocol exchanges and means to establish IP internet protocol packet filtering through an IP internet protocol filter module and state information for the HTTP server to control the terminal device access during and after IEEE 802.1x based authentication process if the access point detects that the terminal device is an IEEE 802.1x client.

14. (original) A method for controlling access by a terminal device in a wireless local area network by determining whether the terminal device utilizes an IEEE 802.1x protocol comprising the steps of:

an access point communicating to the mobile terminal a request to identify, and if the terminal device utilizes an IEEE 802.1x protocol, acknowledging the request to identify, otherwise the access point determining that the terminal is not IEEE 802.1x compliant and selecting an authentication mechanism compatible with the mobile terminal.

15. (currently amended) The method according to claim 14, wherein the access point determines that the terminal is not IEEE 802.1x compliant when it does not receive an ~~EAP~~ extensible authentication protocol identity response packet after a timeout value.

16. (currently amended) The method according to claim 15, further comprising the step of access point detecting that if the terminal device is not IEEE 802.1x compliant, then configuring an ~~IP~~ internet protocol packet filter and redirecting a user HTTP request to a local server.

17. (original) The method according to claim 16, further comprising the step of the local server communicating to the terminal device information specifically related to a browser based authentication.

18. (original) The method according to claim 17, further comprising the step of the access point transitioning to a state if the terminal device utilizes the IEEE 802.1x protocol that indicates that the terminal device is IEEE 802.1x compliant and thereafter processing all communication utilizing the IEEE 802.1x protocol.

19. (original) The method according to claim 17, further comprising the step of the access point transitioning to a state corresponding to browser based authentication if the authentication process fails.

20. (original) The method according to claim 14, further comprising the step of the access point transitioning to a state corresponding to browser based authentication if the terminal device is not IEEE 802.1x compliant.

21. (currently amended) A method for controlling access of a terminal device in a ~~WLAN~~ wireless local area network by determining whether the terminal device utilizes an IEEE 802.1x protocol comprising the steps of: communicating through the an access point to the mobile terminal a request to identify, and if the terminal device utilizes an IEEE 802.1x protocol, acknowledging the request to identify, otherwise determining by the access point that the terminal is not IEEE 802.1x compliant and selecting an authentication mechanism compatible with the terminal.

22. (currently amended) The method according to claim 21, further comprising the step of deter-mining in the access point that terminal is not IEEE 802.1x compliant if it does not receive an ~~EAP~~ extensible authentication protocol identity response packet after a preset time.

23. (currently amended) The method according to claim 21, further comprising the step of detecting in the access point that if the terminal device is not IEEE 802.1x compliant, then configuring an ~~IP~~ internet protocol packet filter and redirecting a user HTTP request to a local server.

24. (original) The method according to claim 23, further comprising the step of communicating from the local server to the terminal device, information specifically related to a browser based authentication.

25. (original) The method according to claim 21, further comprising the step of transitioning to a state in the access point if the terminal device utilizes the IEEE 802.1x protocol that indicates that the terminal device is IEEE 802.1x compliant and thereafter processing all communication utilizing the IEEE 802.1x protocol.

26. (original) The method according to claim 25, further comprising the step of transitioning to a state in the access point corresponding to browser based authentication if the authentication process fails.

27. (original) The method according to claim 21, further comprising the step of transitioning to a state in the access point corresponding to browser based authentication if the terminal device is not IEEE 802.1x compliant.